基于直方图移位的 AMBTC 域无损信息隐藏 *

张 弢[1a]，柳雨农[1a†]，邢亚林[1a]，任 帅[1b]，张德刚[2]

(1. 长安大学 a. 电子与控制工程学院; b. 信息工程学院, 西安 710068; 2. 云南电网有限责任公司 教育培训评价中心, 昆明 650033)

摘 要：针对秘密信息的安全传输，提出了一种信息隐藏算法，将混沌置乱变换及行程压缩编码同时应用于秘密信息预处理，旨在改善隐藏载体的嵌入容量和鲁棒。该算法将直方图移位技术应用于信息嵌入过程，在绝对矩阵块截断编码（AMBTC）生成的高低平均值序列上隐藏预处理后的秘密信息，实现了载体的无损隐藏并提升了嵌入容量，且嵌入容量高于直接在由 AMBTC 生成的高低平均值序列上进行隐藏的算法。实验结果表明，在受到某些攻击后仍保证提取出的秘密信息具有较高的可辨识度，归一化系数始终高于 0.6，证明了该算法在鲁棒性和隐藏效率方面的优势。因此，提出的信息隐藏方法能达到秘密信息安全传输的目的，同时具有很好的抗攻击性。

关键词：信息隐藏；混沌置乱变换；行程压缩编码；绝对矩阵块截断编码

中图分类号：TP309.2 doi: 10.3969/j.issn.1001-3695.2018.01.0006

Lossless information hiding in AMBTC domain based on histogram shift

Zhang Tao[1a], Liu Yunong[1a†], Xing Yalin[1a], Ren Shuai[1b], Zhang Degang[2]

(1. *a. School of Electronic & Control Engineering*, *b. School of Information Engineering*, *Chang'an University*, *Xi'an* 710064, *China*; 2. *Education Training Evaluation Center Yunnan Power Grid Co*, *Kunming* 650033, *China*)

Abstract: For the secure transmission of confidential information, this proposed an information hiding algorithm. Using chaos scrambling transform and run-length code compression simultaneously in the secret information preprocessing, in order to improve the embedding capacity and robustness of the stego. In order to achieve the lossless hiding and improve the capacity, it used the histogram-shift technology and the AMBTC (Absolute Moment Block Truncating Coding) to hide the preprocessed secret information in high and low mean value sequence, and the capacity was larger than that of the algorithm which is only based on the AMBTC. The experimental results show that the extracted secret information can be highly identified even after some attacks, and the normalization coefficient is always lager than 0.6, which proves the advantages of the proposed algorithm in terms of robustness and hiding efficiency. Therefore, the method of information hiding in this paper achieves the goal of secure transmission of secret information and has good anti-aggression.

Key words: information hiding; chaotic scrambling transform; stroke compression coding; AMBTC

0 引言

信息隐藏的主要方式是修改载体数据进行隐藏，旨在将密文隐藏在普通载体中。近年来高嵌入容量与无损恢复的信息隐藏研究广泛应用于医学图像、遥感图像、军事图像等领域。而无损信息隐藏主要面临在数字媒体中实现较大容量的嵌入，实现较低失真的无损信息隐藏、嵌入率及嵌入算法的安全性、传输过程中出现信息丢失和噪声影响等方面的挑战。目前主要载体为二维图像、三维模型、视频、音频等。在二维图像中实现指纹、人脸等特征的信息隐藏已成为安全通信、电子商务及远程身份认证的最新应用技术。Ker 等人[1]提出多幅二维图像信息隐藏方式，该方式对算法计算复杂度极具考验，相反 Qian 等人[2]提出的单幅信息隐藏，简化了算法过程。

秘密信息的预处理作为安全隐藏的前提，置乱与压缩为主要处理方式，文献[3,4]将混沌置乱应用于信息隐藏的图像预处理，文献[5,6]提出改进的 JPEG 图像压缩算法来增加载体的嵌

收稿日期：2018-01-09；**修回日期：**2018-03-13 **基金项目：**国家自然科学基金青年项目（61702050）；陕西省自然科学基础研究计划项目（2014JM2-6105）；中国博士后科学基金资助项目（2015M572510）；陕西省博士后科学基金资助项目；西藏自治区自然科学基金项目（2015ZR-14-20）；长安大学中央高校基本科研业务费专项资金资助（310832151092）；国家级大学生创新创业训练计划项目资助（201510710044）

作者简介：张弢（1984-），女，山西吕梁人，副教授，博士，主要研究方向为模式识别与智能控制、信息隐藏等；柳雨农（1993-），男，甘肃平凉人，硕士研究生，主要研究方向为模式识别与智能控制（1638624145@qq.com）；邢亚林（1993-），男，山东临沂人，硕士研究生，主要研究方向为模式识别与智能控制；任帅（1982-），男，山西太原人，副教授，博士，主要研究方向为信息隐藏以及数字水印技术、信息安全风险评估技术；张德刚（1982-）男，云南临沧人，博士，主要研究方向为数字图像处理.

入容量，文献[7]中提出的基于 Arnold 的置乱算法，该算法具有周期性缺点，破译者很容易掌握其规律并且破译。由于一般的预处理算法基于离散余弦变换的编码算法，在量化中易产生数据缺失和方块效应[8]，此类处理算法只保证了载体的视觉质量，但对载体数据特性产生破坏，攻击者可根据直方图异常、JPEG 分块效应等异常现象有效击破此类隐藏方法[9-10]。针对上述问题，无损信息隐藏(lossless information hiding)能有效地避免破坏原始载体信息，可以完全无损恢复原载体图像，提高信息传输的隐蔽性。Chen 等人提出了由绝对矩阵块截断编码[11,12]（absolute moment block truncating coding，AMBTC）生成高低平均值进行处理的信息隐藏算法，只改变了高低平均值的相对位置。

本文在 AMBTC 无损嵌入算法基础上，对高低平均值数据分别进行直方图移位操作，实现两级无损数据隐藏。首先采用 Chebyshev 映射的混沌置乱及行程压缩编码对密文进行预处理，加强了嵌入系统安全性并具有较好的去相关性；相对于文献[6]的 JPEG 图像压缩，行程编码的压缩比达到 26，对于文献[7]，混沌置乱避免了周期性的缺点。随后采用基于直方图移位的 AMBTC 无损嵌入算法实现信息隐藏，并对隐藏载体进行攻击测试，提取出秘密信息并将归一化系数与文献算法进行对比分析，结果显示本文中算法面临几何攻击和空间滤波攻击具有良好的鲁棒性。因此，本文提出的信息隐藏系统实现秘密信息的安全传输，而且具有较好的抗攻击性。

1 信息隐藏系统组成

本文采用某二值指纹图像作为隐秘信息，图 1、2 为信息隐藏系统的嵌入和检测两过程，隐秘信息与隐藏载体经过隐藏算法形成隐秘载体，视觉上与嵌入之前的载体图像无差别，其次对隐藏载体进行攻击测试，分别提取出隐秘信息和载体图像并与原始图像数据对比，检验其隐藏算法鲁棒性。

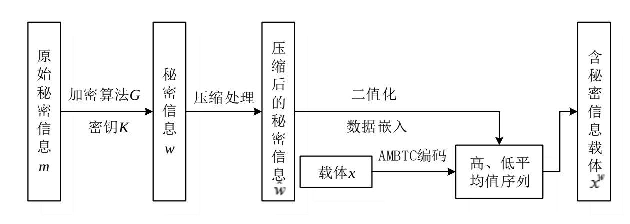


图 1 秘密信息嵌入系统框图

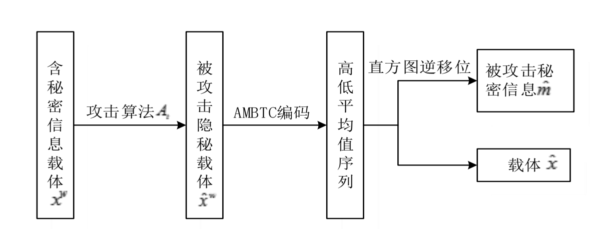


图 2 秘密信息提取系统框图

信息隐藏系统基本包括以下元素：定义 M 为原始隐秘信息 m 的集合；X 为隐藏载体 x 集合；W 为预处理后的隐秘信息 w 集合；K 为隐藏密钥 k 集合；G 表示利用原始信息 m、密钥 k 及隐藏载体 x 生成的加密算法：

$$G: M\times X\times K\rightarrow W, w=G(m,x,k) \tag{1}$$

A_t 表示对嵌入隐秘信息的载体 x^w 攻击测试算法:

$$A_t: X\times K\rightarrow X, \hat{x}=A_t\left(x^w, K'\right) \tag{2}$$

2 置乱算法

2.1 Chebyshev 映射

Chebyshev 映射与 Logistic 映射、Henon 映射同属于混沌置乱算法，由 Chebyshev 提出的以阶数为参数的混沌映射。设 C[-1,1] 上的所有实值连续函数构成的向量空间，则 $\{\cos(n\arccos\chi_n), n\in[0,\infty)\}$ 是 C[-1,1] 上的一组基。令 $T_n(\chi)=\cos(n\arccos\chi_n)$，则 $T_n(\chi)$ 称为 n 阶第一切比雪夫多项式。当迭代次数为 k，Chebyshev 映射如下：

$$x_{n+1}=\cos(k\arccos x_n) \tag{3}$$

其中: $x_n\in(-1,1)$，当 $k\geq 2$ 时，映射进入混沌区域。

基于 Chebyshev 映射的置乱算法

算法 1 置乱算法

a)获取混沌随机序列 $X=\{x_1, x_2\cdots x_{8m\times n}\}$，经过对(2.1) 迭代 $8m\times n$ 次，m、n 为图像宽、高。

b) 从随机序列 X 中选取 8 个数得到一个序列 $Y=\{y_1, y_2\cdots y_8\}$。

c)将序列 Y 经过一次置换得 $Y'=\{y'_1, y'_2\cdots y'_8\}$。

d)获取一个索引序列 D_i，$D_i=\{d_1, d_2, \cdots d_8\}$，其中 d_i 表示 D_i 序列中第 i 个数在 Y'_i 的位置。

算法 2 Chebyshev 映射 N 次迭代算法

a)获取二进制序列 $K_i=\{k_1, k_2\cdots k_8\}$，将秘密信息转换一维序列 $G_i=\{g_1, g_2\cdots g_{8m\times n}\}$，将 g_i 转换为 K_i。

b)利用算法 1 得到的索引序列 D_i 对 B_i 进行置换，得到序列 $K'_i=\{k'_1, k'_2\cdots k'_8\}$。

c)将序列 K'_i 转换成 g'_i。

d)重复步骤 b)c)4 $m\times n$ 次。

e)得到 N 次迭代序列 $G'_i=\{g'_1, g'_2\cdots g'_{8m\times n}\}$。

2.2 混沌置乱算法检验

对 Chebyshev 映射的混沌置乱算法进行仿真，Matlab2012 仿真环境中，选取大小为 512×512 的指纹图像。其中图（a）为原始图像，（b）为混沌置乱图像，（c）为反置乱变换后图像，（d）为原始图像直方图，（e）为混沌置乱图像直方图，（f）为反置乱变换后图像直方图：

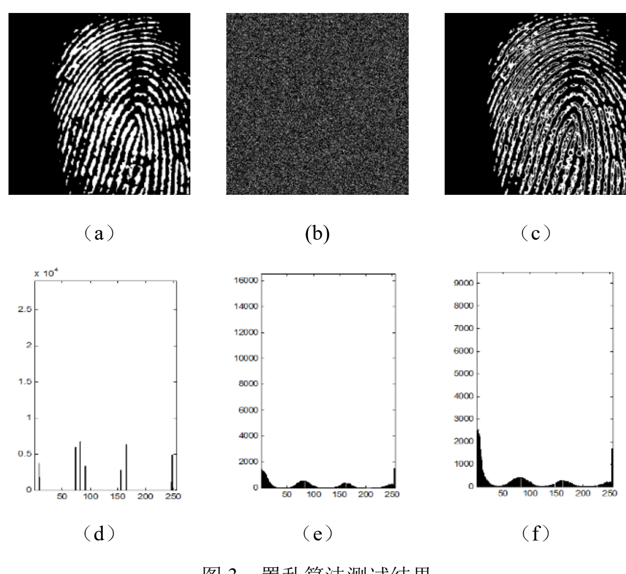


图 3 置乱算法测试结果

在混实验结果中，图（a）~（c）体现出混沌置乱算法具有极好的置乱效果，置乱改变了原图像的数据，再经过反置乱变换后，置乱图像恢复原始画面，在直方图（d）~（f）中，对图像数据进行比较，可得到当秘密图像经过置乱与反置乱变换得到的恢复图像，其图像的亮度变暗，图像数据发生改变但不改变图像内容。

3 压缩算法理论

本文提出压缩编码来减少隐秘信息在嵌入载体的数据量，由于图像的冗余性和相关性，图像压缩的本质是对图像数据按照一定规则进行变换和组合，来去除冗余信息量。信息量与信息熵组成了该压缩算法的理论。

3.1 信息量

设一个信息源 X 发出的一个信息元素集合表示为 $A=\{a_i|i=1,2,...,m\}$，X 发出的 a_i 出现概率为 $p(a_i)$，则定义元素 a_i 出现的信息量为

$$I(a_i)=-\log_2 p(a_i) \tag{4}$$

3.2 信息熵

对信息源 X 各元素自信息量取统计平均，得每个元素平均自信息量 $H(X)$，称为信息源的熵，定义为

$$H(X)=-\sum_{i=1}^{m} p(a_i)\log_2 p(a_i) \tag{5}$$

在式（5）中，若图像灰度级为[1,M]，通过直方图各灰度级出现的概率为 $p_s(s_i), i=1,2,...,M$，得到图像的熵为

$$H=-\sum_{i=1}^{m} p(s_i)\log_2 p_s(s_i) \tag{6}$$

通常，以峰值信噪比 PSNR 作为客观评价指标，表示为

$$PSNR=10\lg\frac{(L-1)^2}{(e_{rms})^2} \tag{7}$$

其中：L 是图像灰度级总数，e_{rms} 表示大小为 $M\times N$ 的图像的均方误差，其定义如下：

$$e_{rms}=\sqrt{\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left[\hat{f}(x,y)-f(x,y)\right]^2} \tag{8}$$

隐藏信息的数据压缩处理使用一种无损压缩编码，即行程编码（run-length code compression，RLCC），选取大小为 512×512 的灰度图作为同样的测试图像，图（a）为密文的原始图像二值图，图（b）为压缩后结果，图（c）为解压后图像；图（d）~（f）为原始图、压缩图像、解压后图像数据，测试结果如下：

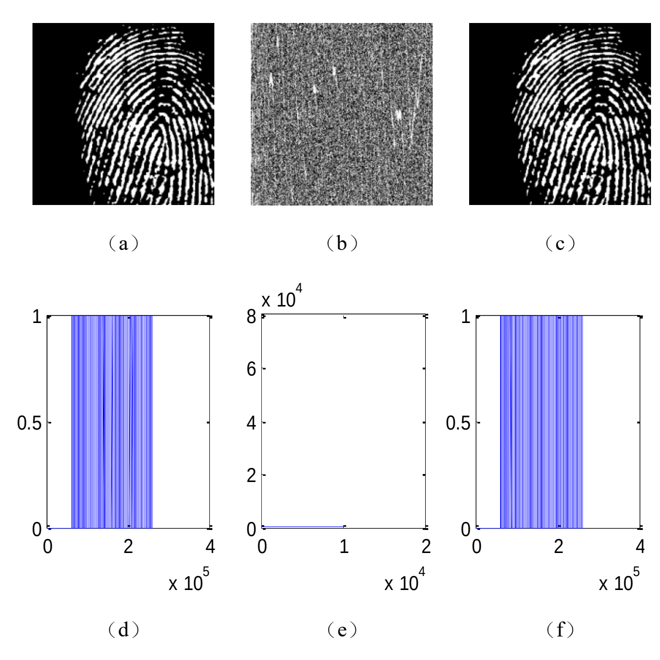


图 4 压缩编码算法测试结果

霍夫曼编码算法编码时间为 103 t，压缩比为 1.7，而 RLCC 的编码时间为 1.7 t（t 为单位时间 s），压缩比为 26.2。可见，RLCC 算法复杂度简单且压缩速率优于霍夫曼编码。

4 嵌入算法理论

隐藏信息嵌入作为信息隐藏系统的核心，面临着在传输过程中被攻击的挑战，因此对抗攻击性要求较高。在此之前，Lema 和 Mitchell 提出了 AMBTC 编码嵌入算法，而 Chen 等人[11,12]后来在此基础上引入了直方图移位，但此方法对直方图移位具有依赖性的数据改变而无法恢复。面对以上问题，这里提出了一种基于直方图移位的 AMBTC（绝对矩阵块截断编码）高低均值压缩图像隐写嵌入方法，其过程简化为两个步骤：用数据替换二进制位图和根据所嵌数据和原始位图最优化高低均值。

4.1 数据嵌入

a)AMBTC 编码。设一幅大小为 $M\times N$ 的图像 C，取块大小为 $m\times n$，经 AMBTC 编码得到高低平均序列，l_i 和 h_i 表示高低序列块元素：

$$L=\{l_i|1\le i\le (M\times N)/(m\times n)\} \tag{9}$$

$$H=\{h_i|1\le i\le (M\times N)/(m\times n)\} \tag{10}$$

以及位平面

$$B=\{B_i|1\le i\le (M\times N)/(m\times n)\} \tag{11}$$

其中 B_i 大小为 $m\times n$，且与 l_i 和 h_i 构成三元组（l_i,h_i,B_i）。

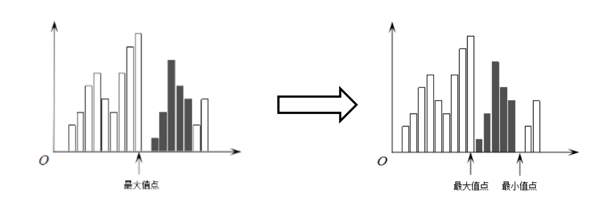


图 5　直方图移位示意图

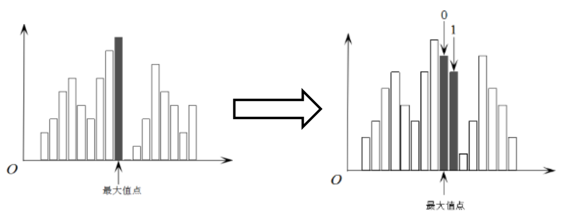


图 6　数据嵌入示意图

b)高平均序列直方图移位。

（a)计算平均序列进行直方图移位：$H_h(x), x\in[0,255]$。

(b)在 $H_h(x)$ 中找到最大值点 $x_{\max}$ 和最小值点 $x_{\min}$，假设 $x_{\max}<x_{\min}$ 的情况，如图 6 所示。若 $H_h(x)\ne 0$ 记录所有值等于 $x_{\min}$ 的像素点位置。

(c)移位（图 5）：若 $x_{\max}>x_{\min}$，遍历整个序列 H，当 $h_i\in[x_{\max}+1,x_{\min})$ 时，进行（h_i+1）；若 $x_{\max}<x_{\min}$，当 $h_i\in(x_{\min},x_{\max}-1]$ 时，进行（h_i+1）。

(d)嵌入数据；再次遍历序列 H，当 $h=x_{\max}$ 时，若嵌入的数据为“1 ”，则将 h_i 进行加 1；若嵌入数据为“0”，则 h_i 不变。

c)如同步骤 b)，对低平均序列 L 进行直方图移位。

d)修改高低平均值的相对次序：遍历经过直方图移位后的高低平均值序列 H' 和 L'，当 $h_i'\ne l_i'$ 时，如果待嵌入数据为“1”，交换 l_i' 和 h_i' 位置。同时，将 l_i' 和 h_i' 对应的 B_i 中所有比特位翻转；如果嵌入数据为“0”，保持（l_i,h_i,B_i）不变。在 $h_i'=l_i'$ 时，直接将 $m\times n$ 位的待嵌入数据替换 B_i。

4.2 数据提取与图像恢复

数据的提取和图像恢复为数据嵌入的逆过程。

a)统计高低平均值序列的相对次序。遍历隐藏数据高低平均值序列 H^W 和 L^W，在 $h_i^W\ne l^W{}_i$ 时，如果 $h_i^W<l^W{}_i$，提取数据“1”，并交换 l_i^W 和 h_i^W 位置。同时，将 l_i^W 和 h_i^W 对应的 B_i 中所有比特位翻转；如果 $h_i^W>l^W{}_i$，提取出数据“0”，保持(l_i,h_i,B_i)不变。在 $h_i^W=l_i^W$ 时，直接从 B_i 中将 $m\times n$ 位的待嵌入隐藏数据提取出来。

b)对低平均值序列进行直方图逆过程如下：

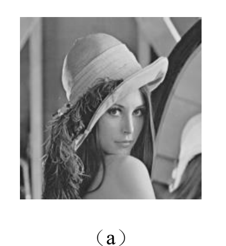
(a)提取数据。按照步骤 a)处理后的低平均值序列 L''。若 $x_{\max}>x_{\min}$，则当 $l_i''=x_{\max}+1$ 时，提取出数据“1”，然后将 l_i'' 减 1；若 $l_i''=x_{\max}$，则提取数据“0”。若 $x_{\max}<x_{\min}$，则当 $l_i''=x_{\max}-1$ 时，提取数据“1”，然后将 l_i'' 减 1；若 $l_i''=x_{\max}$，则提取出的数据为“0”。

(b)数据恢复。再次按顺序遍历低平均值序列 L''。若 $x_{\max}>x_{\min}$，则当 $l_i''\in(x_{\max}+1,x_{\min})$，将 l_i'' 减 1。若 $x_{\max}<x_{\min}$，则当 $l_i''\in[x_{\min},x_{\max}-1)$，将 l_i'' 减 1。若 $H_l(x_{\min})\ne 0$，然后根据记录相应位置像素置为 $x_{\min}$。

c)对低平均值进行直方图移位逆过程。按照步骤 b）对高平均值 H'' 进行操作。

4.3 实验结果

实验中，采用“Lena”、“Bridge”、“Dollar”三幅大小为 512×512 的 256 阶灰度图像进行测试，如图 7 所示。图 9 为编码所得到的最高、最低平均值序列，图 8 为 ATMBTC 编码生成的位平面，在 ATMBTC 编码后的载体图像中嵌入图 4 经过预处理的秘密图像，其嵌入信息后结果如图 10 所示。


（a）

（b）

（c）

图 7　原始载体图像


（a）

（b）

（c）

图 8　AMBTC 生成的位平面



图 9　a.b.c 为 AMBTC 生成的低平均值序列；
d.e.f 为 AMBTC 生成的高平均值序列

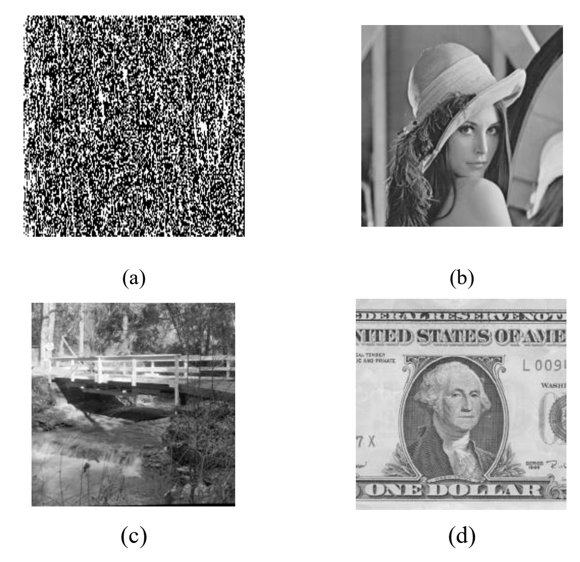


图 10　a 为预处理后的秘密图像，b.c.d 为含密载体

表 1　算法性能比较

图像	Lena	Bridge	Dollar
AMBTC 算法 PSNR（dB）	32.140	28.685	30.021
本文提出的算法 PSNR（dB）	32.131	28.653	30.014
Chen 等人算法 PSNR（dB）	32.140	28.685	30.021
本文算法恢复图像 PSNR（dB）	32.131	28.653	30.014
本文算法嵌入容量（Bits）	16762	17567	16878
Chen 等人算法嵌入容量（Bits）	16414	17194	16544

在表 1 的实验结果中，可看出本文中直方图移位技术较 Chen 等人提出算法在嵌入容量有所提升，而 Chen 等人算法相比 AMBTC 编码嵌入算法在性能上较优，且出现在“Lena”“Bridge”载体图像的嵌入容量高于 16384（128×128），主要由于这两幅图像中存在一些高低平均值相等的块。恢复后的载体图像与嵌入信息前的载体图像的 PSNR 都为 32.131，表明秘密信息在未受攻击情况下，提取之后载体图像恢复完整，从而达到无损信息隐藏目的。

5　鲁棒性实验

信息隐藏算法的抗攻击性实际是对鲁棒性进行检验，对图像进行空间滤波、有损压缩、几何变形等攻击，检验提取出秘密信息的恢复程度，这里用提取出秘密信息与原始信息的归一化相关系数作为评估算法鲁棒性的标准，可表示如下：

$$NC=\frac{\sum_{i}^{N} w_i \hat{w}_i}{\sqrt{\sum_{i}^{N} w_i^2}\sqrt{\sum_{i}^{N} \hat{w}_i^2}}\begin{cases}\geq T, 存在秘密信息 w\\ \leq T, 不存在秘密信息 w\end{cases} \tag{12}$$

其中：T 为预先设定的阈值，经实验，设 T 定值为 0.6。

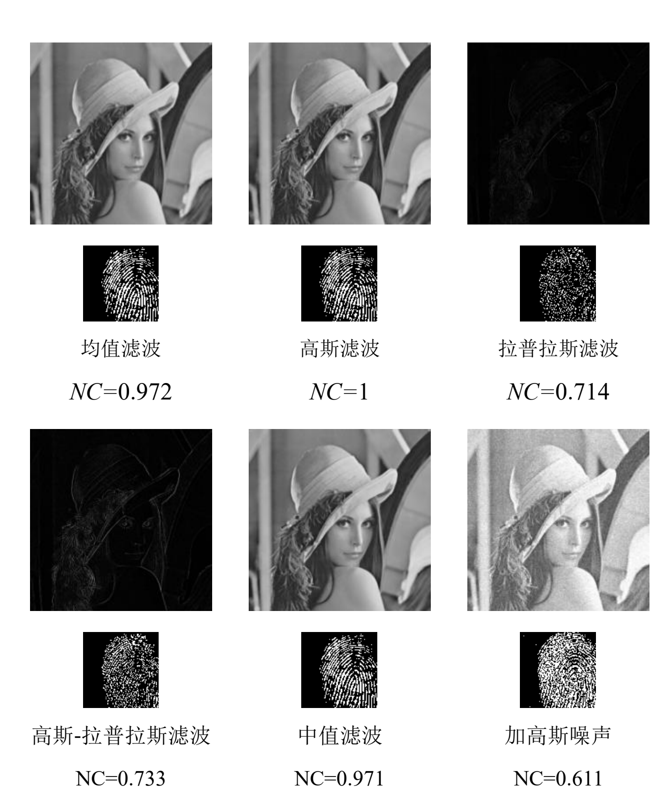


图 11　空间滤波攻击实验

从空间滤波攻击的检测实验结果得出，经过预处理秘密信息，在受到空间滤波攻击后的 NC 值仍大于 0.6，可看出本文提出的隐藏算法可以有效地抵抗空间滤波攻击和高斯噪声攻击，而且面临高斯滤波攻击时归一化系数最大为 1，即对高斯滤波的攻击该算法具有完全抵抗的性能，且对于中值、均值滤波攻击时有很好的鲁棒性，但对与高斯噪声的攻击时鲁棒性相对较弱，因此接下的工作可以针对本文算法噪声攻击时提高鲁棒性。

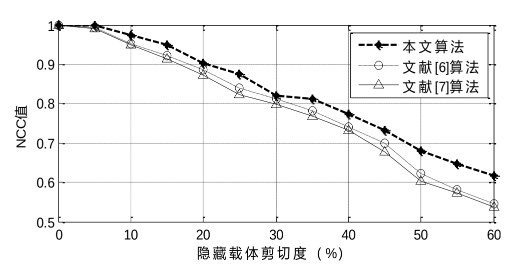


图 12　剪切攻击算法性能比较曲线

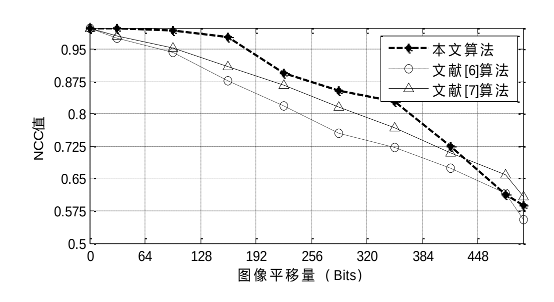


图 13 图像平移攻击算法性能对比曲线

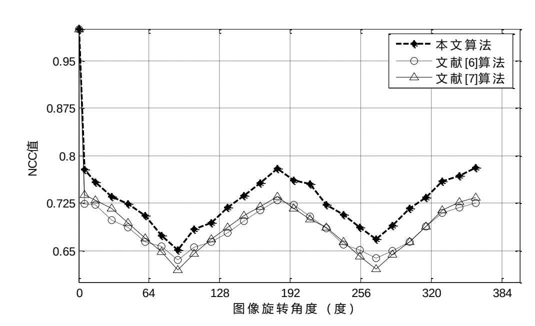


图 14 图像旋转攻击算法性能对比曲线

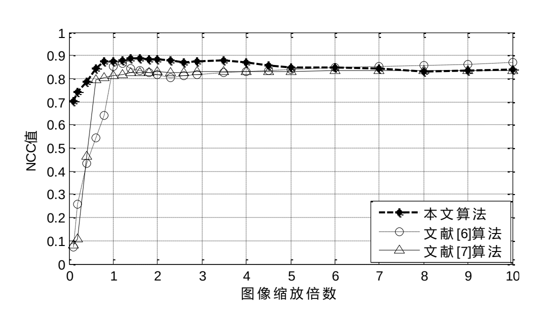


图 15 图像缩放攻击算法性能对比曲线

从图 12 曲线看出，在隐藏载体受到剪切攻击后提取秘密信息，将本文提出算法与文献进行比较，随着剪切度增加到 60%时，本文中算法的 NC 值始终大于阈值 0.6，表现出较强的抗剪切攻击，文献[6，7]算法小于 0.6；图 13 中对于平移攻击测试，当受到平移面积大于 400 时，其 NC 值较差于文献[6]，而且鲁棒性的整体稳定性不及文献[6、7]的算法；图 14 中受到旋转攻击测试时 NC 值高于 0.65 且有一定的规律性，而且抗旋转性能优于文献[6,7]；图 15 中的缩放攻击算法鲁棒性比较时，本文算法 NC 大于 0.7，且在缩放倍数为 1 时达到最大 0.886，当缩放倍数大于 2 时，NC 值理想且保持稳定。实验表明，本文中隐藏算法在图像剪切、旋转以及缩放攻击时表现出较强的鲁棒性；当载体图像大面积受到平移攻击时，其鲁棒性较弱。但本文算法的整体抗攻击性能及其鲁棒性较好。

6 结束语

本文采用对秘密图像进行混沌置乱及行程编码的预处理，具有加密隐藏信息并减小嵌入数据的效果，采用基于直方图移位的 AMBTC 无损信息隐藏算法嵌入秘密信息，达到一定的视觉冗余，实验中本文算法嵌入容量为 16 762，高于 Chen 等人算法的嵌入容量 16 414，并实现无损信息隐藏。经过算法鲁棒性测试，并与文献[6，7]算法进行比较。实验结果表明，当载体图像受到局部攻击时，隐藏信息可以检测，本文算法性能相对于文献[6，7]具有明显优势，但在大面积被攻击时鲁棒性较差。结果显示，本文提出的信息隐藏方案不仅实现秘密指纹图像的安传输，而且在面临几何攻击与滤波攻击时具有较好的鲁棒性，完整提取出传输的秘密信息。

参考文献：

[1] Ker A, Pevny T. A new paradigm for steganalysis via clustering [C]// Proc of SPIE, Media Watermarking, Security, and Forensics III. 2011: 7880.

[2] Qian Z, Zhou H, Zhang W, Zhang X. Robust steganography using texture synthesis [C]// Proc of the 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 2016.

[3] 刘娟妮，周诠，李小军，方海. 多光谱图像变换域统计量移位鲁棒无损信息隐藏 [J]. 电讯技术，2015, 55 (11): 1187-1193. (Liu Juanni, Zhou Quan, Li Xiaojun, Fang Hai. Statistical shifts of multispectral image transforms with robust lossless information hiding [J]. Telecommunication Engineering, 2015, 55 (11): 1187-1193.)

[4] 张怡，王慧琴. 基于混沌置乱的小波域数字水印算法研究 [J]. 电脑知识与技术，2011, 7 (10): 2400-2402. (Zhang Yi, Wang Huiqin. Research on digital watermarking algorithm based on chaos scrambling in wavelet domain [J]. Computer Knowledge and Technology, 2011, 7 (10): 2400-2402.)

[5] 赵慧民，范九伦. 一种在 JPEG2000 中隐藏指纹图像的方法研究 [J]. 电路与系统学报，2010, 15 (2): 27-32. (Zhao Huimin, Fan Jiulun. Study on the method of hiding fingerprint image in JPEG2000 [J]. Journal of Circuits and Systems, 2010, 15 (2): 27-32.)

[6] 房宜汕. 一种基于 JPEG2000 特性的信息隐藏技术的研究 [J]. 嘉应学院学报，2013, 31 (2): 24-29. (Fang Yiqi. Research on information hiding technology based on JPEG2000 characteristics [J]. Journal of Jiaying University, 2013, 31 (02): 24-29.)

[7] 张海涛，姚雪，陈虹宇，等. 基于分层 Arnold 变换的置乱算法 [J]. 计算机应用，2013, 33 (8): 2240-2243. (Zhang Haitao, Yao Xue, Chen Hongyu, Zhang Hao. Scrambling algorithm based on hierarchical Arnold transform [J]. Journal of Computer Applications, 2013, 33 (8): 2240-2243.)

[8] Tang Meng S, Chen X, *et al.* An adaptive image steganography using AMBTC compression and interpolation technique [J]. Optik: International Journal for Light and Electron Optics, 2016, 127 (1): 471-477.

[9] 黄蕊蕊，闫肃，解成俊，等. 基于 JPEG_LS 的图像无损信息隐藏方法 [J]. 北华大学学报：自然科学版，2015, 16 (2): 276-280. (Huang Ruirui, Yan Su, Xie Chengjun, Xu Xiaolong. Image lossless information hiding method based on JPEG_LS [J]. Journal of Beihua University: Natural Science, 2015, 16 (2): 276-280.)

[10] Prameelamma M, Sridhar V, Nagendra G, *et al.* AMBTC-compressed images for lossless steganography [J]. International Journal of Advanced

Research in Computer Science & Electronics Engineering, 2012, 1 (6) .

[11] Chen J, Hong W, Chen T S, *et al.* Steganography for BTC compressed images using no distortion technique [J]. Imaging Science Journal the, 2010, 58 (4): 177-185.

[12] An oblivious fragile watermarking scheme for images utilizing edge transitions in BTC bitmaps [J]. Science China: Information Sciences, 2012, 55 (11): 2570-2581.

[13] 张新鹏，钱振兴，李晟. 信息隐藏研究展望 [J]. 应用科学学报，2016 (5): 475-489. (Zhang Xinpeng, Qian Zhenxing, Li Wei. Prospects of information hiding research [J]. Journal of Applied Sciences, 2016 (5): 475-489.)